BCH符号（その３）

情報数理学特別講義I 第9回

2025-11-06

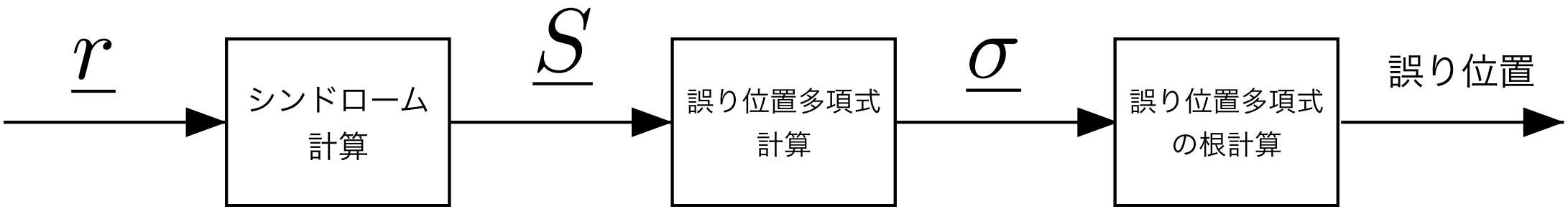
前回の講義

- BCH符号の定義，生成多項式の設計法
  - 原始元 α に対して，$\alpha, \alpha^2, \ldots, \alpha^{2t}$ を根にもつ生成多項式 $g(x)$ で定義される長さ $2^q - 1$ の2元符号
  - $g(x) = \mathrm{LCM}\{\mu_\alpha(x), \mu_{\alpha^3}(x), \ldots, \mu_{\alpha^{2t-1}}(x)\}$
- $t = 1, 2$ の誤り訂正手順.

$t = 3$ の場合

$t = 2$ の訂正方法と同様に，下記の2元BCH符号手順に従い説明する．

1. 誤りを含む可能性のある受信語 $\underline{r}$ を入力し，シンドローム $\underline{S}$ を計算する．
2. シンドローム $\underline{S}$ から，誤り位置多項式 $\sigma(x)$ を求める．
3. 誤り位置多項式 $\sigma(x)$ の根を計算する．



シンドロームの計算 $(t = 3)$

$t = 3$ の2元BCH符号の生成多項式は $\alpha, \alpha^3, \alpha^5$ を根に持つ.
よって3つのシンドローム S_1, S_3, S_5 を計算することができる.
いま，$i+1, j+1, l+1$ビット目に誤りが発生したとする．このときのエラー多項式は
$e(x) = x^i + x^j + x^l$ となる．よって得られるシンドロームは

$$
\begin{aligned}
S_1 &= \alpha^i + \alpha^j + \alpha^l, \\
S_3 &= \alpha^{3i} + \alpha^{3j} + \alpha^{3l}, \\
S_5 &= \alpha^{5i} + \alpha^{5j} + \alpha^{5l}
\end{aligned}
$$

となる.
このようにして得られた S_1, S_3, S_5 から,
誤り位置多項式 $\sigma(x) = \sigma_0 + \sigma_1 x + \sigma_2 x^2 + x^3$ を求める.

$t = 3$ のときの ELP

命題 10.1

$t = 3$ のときの誤り位置多項式 $\sigma(x) = \sigma_0 + \sigma_1 x + \sigma_2 x^2 + x^3$ の係数 $\sigma_0, \sigma_1, \sigma_2$ は

$$\sigma_0 = \frac{S_3(S_1^3 + S_3) + S_1(S_1^5 + S_5)}{S_1^3 + S_3},$$

$$\sigma_1 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3},$$

$$\sigma_2 = S_1$$

となる.

証明

x^2 の係数 σ_2 は，$\sigma(x) = (x+\alpha^i)(x+\alpha^j)(x+\alpha^l)$ より S_1 となることは明らか.

$$\sigma(x) = \sigma_0 + \sigma_1 x + S_1 x^2 + x^3.$$

この誤り位置多項式に $\alpha^i, \alpha^j, \alpha^l$ を代入したものを計算すると

$$\begin{aligned} \sigma_0 + \sigma_1\alpha^i + S_1\alpha^{2i} + \alpha^{3i} &= 0 \\ \sigma_0 + \sigma_1\alpha^j + S_1\alpha^{2j} + \alpha^{3j} &= 0 \\ \sigma_0 + \sigma_1\alpha^l + S_1\alpha^{2l} + \alpha^{3l} &= 0 \end{aligned} \tag{10-1}$$

この3つの式を両辺で足すと

$$\begin{aligned} &\sigma_0 + \sigma_1(\alpha^i + \alpha^j + \alpha^l) + S_1(\alpha^{2i} + \alpha^{2j} + \alpha^{2l}) + (\alpha^{3i} + \alpha^{3j} + \alpha^{3l}) = 0 \\ &\sigma_0 + \sigma_1 S_1 + S_1^3 + S_3 = 0 \end{aligned} \tag{10-2}$$

次に，式 (10-1) の3つの式に，それぞれ $\alpha^{2i}, \alpha^{2j}, \alpha^{2l}$ を掛けると

$$\sigma_0\alpha^{2i} + \sigma_1\alpha^{3i} + S_1\alpha^{4i} + \alpha^{5i} = 0$$
$$\sigma_0\alpha^{2j} + \sigma_1\alpha^{3j} + S_1\alpha^{4j} + \alpha^{5j} = 0$$
$$\sigma_0\alpha^{2l} + \sigma_1\alpha^{3l} + S_1\alpha^{4l} + \alpha^{5l} = 0$$

この3つの式を両辺で足すと

$$\begin{aligned}
&\sigma_0(\alpha^{2i} + \alpha^{2j} + \alpha^{2l}) + \sigma_1(\alpha^{3i} + \alpha^{3j} + \alpha^{3l}) \\
&+ S_1(\alpha^{4i} + \alpha^{4j} + \alpha^{4l}) + (\alpha^{5i} + \alpha^{5j} + \alpha^{5l}) = 0 \qquad (10\text{-}3) \\
&\sigma_0 S_1^2 + \sigma_1 S_3 + S_1^5 + S_5 = 0
\end{aligned}$$

式 (10-2), (10-3) に対して定数項を移項して，並べると

$$\sigma_0 + \sigma_1 S_1 = S_1^3 + S_3$$
$$\sigma_0 S_1^2 + \sigma_1 S_3 = S_1^5 + S_5$$

行列の形式で書くと

$$\begin{pmatrix} 1 & S_1 \\ S_1^2 & S_3 \end{pmatrix} \begin{pmatrix} \sigma_0 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_1^3 + S_3 \\ S_1^5 + S_5 \end{pmatrix}$$

逆行列を計算すると

$$\begin{pmatrix} \sigma_0 \\ \sigma_1 \end{pmatrix} = \frac{1}{S_1^3 + S_3} \begin{pmatrix} S_3 & S_1 \\ S_1^2 & 1 \end{pmatrix} \begin{pmatrix} S_1^3 + S_3 \\ S_1^5 + S_5 \end{pmatrix}$$

以上より，命題10.1が証明された．□

ELPの導出に関して

以上のように，誤り数 $t = 3$ に対しても誤り位置多項式 $\sigma(x)$ を計算することができる.
任意の誤り数 t に対しても同様に誤り位置多項式 $\sigma(x)$ を計算することはできるが，解くべき逆行列が大きくなっていくため計算するのが難しくなる.
専門書においても，$t = 5$ までの計算式しか書かれていない.

練習問題1(15分)

$GF(2^4)$ の原始元 α の最小多項式 を $\mu_\alpha(x) = 1 + x + x^4$ とする．生成多項式 $g(x) = \mu_\alpha \mu_{\alpha^3} \mu_{\alpha^5}$ で定義された長さ 15 の3誤り訂正2元BCH符号によって符号化された符号多項式が，通信路を通って受信多項式 $r(x) = 1 + x + x^3 + x^5 + x^6$ となったとき，誤り位置に対応する$GF(2^4)$ 上の元を求めよ．

解法手順

(1) シンドローム S_1, S_3, S_5 を計算する．

(2) 誤り位置多項式 $\sigma(x) = \sigma_0 + \sigma_1 x + S_1 x^2 + x^3$ の係数 σ_0, σ_1 はそれぞれ $\sigma_0 = \frac{S_3(S_1^3+S_3)+S_1(S_1^5+S_5)}{S_1^3+S_3}$，　$\sigma_1 = \frac{S_1^2 S_3+S_5}{S_1^3+S_3}$ となる．

(3) $GF(2^4)$ の非零の元を順に $\sigma(x)$ へ代入し，誤り位置多項式の根を求める．

練習問題2(15分)

$GF(2^4)$ の原始元 α の最小多項式 を $\mu_\alpha(x) = 1 + x + x^4$ とする．生成多項式 $g(x) = \mu_\alpha \mu_{\alpha^3} \mu_{\alpha^5}$ で定義された長さ 15 の3誤り訂正2元BCH符号によって符号化された符号多項式が，通信路を通って受信多項式 $r(x) = 1 + x^3 + x^4 + x^6 + x^8 + x^9$ となったとき，誤り位置に対応する$GF(2^4)$ 上の元を求めよ.

解法手順

(1) シンドローム S_1, S_3, S_5 を計算する.

(2) 誤り位置多項式 $\sigma(x) = \sigma_0 + \sigma_1 x + S_1 x^2 + x^3$ の係数 σ_0, σ_1 はそれぞれ $\sigma_0 = \frac{S_3(S_1^3+S_3)+S_1(S_1^5+S_5)}{S_1^3+S_3}$，　$\sigma_1 = \frac{S_1^2 S_3+S_5}{S_1^3+S_3}$ となる.

(3) $GF(2^4)$ の非零の元を順に $\sigma(x)$ へ代入し，誤り位置多項式の根を求める.